

### ***1. Section 316.2 – Definitions***

*c. Should opt-out obligations be extended to third-party list providers who do nothing more than provide a list of names to whom others send commercial emails? If so, how could this be accomplished, given the statutory language which defines “sender” in terms of an entity that both initiates a message and advertises its product, service, or Internet web site in the message?*

It is nearly impossible to identify the source list of an email address when advertisements are sent via email. While the concept of removing an email address from the sender’s list, the advertiser’s list, and the original source list may be appealing to consumers, the reality is that such a requirement is nearly impossible to implement and monitor. Without the ability to reliably track and monitor adherence to such requirements, the rule would be useless.

*d. Should the Commission adopt a “safe harbor” with respect to optout and other obligations for companies whose products or services are advertised by affiliates or other third parties? If not, why not? If so, what would be appropriate criteria for such a safe harbor?*

Adopting safe harbor for companies that advertise products through affiliates would allow advertisers to continuously circumvent CAN SPAM requirements. Some of the worst practices and violations of CAN SPAM and unsubscribe come from advertisers using affiliates who are not taking responsibility for the actions of their affiliates. It is absolutely critical that advertisers using affiliates or affiliate networks share in the responsibility for the actions of their affiliates.

### ***4. Section 316.4 – Prohibition Against Failure To Honor Opt-Out Requests Within Three Business Days Of Receipt***

*a. Is three business days an appropriate deadline for effectuating an opt-out request? If not, what time frame would be more appropriate? Does the Commission’s proposal that multiple advertisers in a single commercial email message may arrange to have only one of those advertisers be the “sender” affect what time frame would be appropriate? If so, how?*

LashBack does not see any advantage of lowering the unsubscribe deadline from 10 business days to 3 business days.

*b. Are some commenters’ concerns warranted that under the original ten-business-day provision senders would be permitted to bombard a recipient with email for ten business days following his or her opt-out request? Why or why not? Is this a commonly-occurring practice? If so, what is the evidence supporting this? Providing as much detail as possible, explain whether recipients continue to receive commercial email from a particular sender after submitting an opt-out to that sender. For example, are recipients who submit opt-out requests targeted for receipt of additional commercial email? How likely are recipients to continue to receive additional commercial email from a particular sender within ten business days after submission of an opt-out request? How likely after ten business days?*

LashBack has seen absolutely no evidence that once an unsubscribe request is submitted that the unsubscribing email is bombarded by emails from the advertiser or sender prior to the ten business day removal period. That said, LashBack has strong data to suggest that compliance with the 10 day removal period is low and only the most respected companies are honoring requests in this time frame.

### ***5. Section 316.5 – Receipt of Requests Not to Receive Future Commercial Email Messages From a Sender***

*b. Does the Commission's proposal regulating how recipients submit opt-out requests accomplish the goal of removing all extraneous encumbrances that could interfere with a recipient's ability to submit an opt-out request? Do any email senders deprive recipients of any benefit when they submit an opt-out request? Should depriving recipients of a benefit when they opt out be added to the list of encumbrances prohibited by this proposal?*

The proposed rules are excellent and will help bring clarity to the fact that there should be minimal steps and requirements for a consumer to submit an opt-out request.

*c. Should the Commission's proposal regulating how recipients submit opt-out requests be changed in any way?*

Even more clarity should be brought to the rule. Specifically, it is very important to ensure that only an email address should be required to unsubscribe. Users should not have to log in to a site (even if they are a member of that site), or have to go through any verification processes, such as image verification or confirming an email unsubscribe through clicking on a link in another email received from the same sender. This practice is all too common and restricts an individual's ability to unsubscribe. Additionally, it restricts outside organizations such as LashBack from monitoring the practices of these parties.

Additionally, it is a common practice for web pages that allow users to unsubscribe to employ technology that not all users or Internet browsers support. Specifically, many unsubscribe pages require that the user's browser support a specific version of JavaScript or allow cookies to be stored. Unlike HTML, these technologies are not universally supported in all types of browsers (Internet Explorer, Netscape, Firefox, Opera, etc). Also, users have the option to disable these items as a personal preference. Any web pages set up for allowing users to unsubscribe should not require technical features that are not supported universally by all browsers. If the unsubscribe page does require these items, then the sender should also provide an alternative mechanism (such as an email address) that does not have specific technology requirements that are not universally supported in all browsers.

Finally, it is all too common for email senders to try to mask their unsubscribe option in email sent. For instance, there are numerous cases where companies will label unsubscribe links as: No more, no way, stop it now, not for me, or use foreign characters in labeling their unsubscribe link, such as Opt0ut, st0p, etc. Additionally, other companies will embed their unsubscribe option in an image. If the user has images disabled in their email client to protect privacy or the image fails to load, then the user has no way of knowing there is an unsubscribe option. Forcing at least some convention on this should reduce the burden placed on consumers. Even simple requirements such as forcing senders and advertisers to place unsubscribe links at the bottom of email sent and labeling them with either SENDER-UNSUBSCRIBE: xxxx@sss.com or ADVERTISER-UNSUBSCRIBE: <http://url.com> would create vast improvements and create some degree of standards. LashBack acknowledges such conventions will not be received well by advertisers and senders, but urges the FTC to force at least some minimal standards in the labeling of unsubscribe options in email sent.

## ***6. Aggravated Violations Relating To Commercial Email***

*c. Are there practices that contribute substantially to the proliferation of unlawful commercial email messages and are not already prohibited by the Act? For example, is harvesting email*



*addresses from peer-to-peer networks already prohibited by the Act? Is that practice contributing substantially to the proliferation of unlawful commercial email messages? Is harvesting email addresses from newsgroups and other similar online forums already prohibited by the Act? Is that practice contributing substantially to the proliferation of unlawful commercial email messages?*

LashBack has thousands of examples of companies that allow their suppression lists to mis-used. These cases indicate that the companies collecting the unsubscribe requests provide these lists to other parties which send even more spam to the list. Whether these actions are intentional or unintentional by the company collecting the unsubscribe request, these actions result in high volumes of spam being sent to the unsubscribing party. LashBack has identified several cases where one unsubscribe request has resulted in several thousand messages being sent to the email address unsubscribing in less than a month's time. It is critical that these cases are properly addressed under CAN SPAM. Since the companies sending email to the addresses in a suppression list are technically not using electronically harvested addresses, their practice may actually be legal under CAN SPAM. If also considering manual harvesting ensures that the companies sending to other company's suppression lists can be held accountable, then this rule should be adopted.

Additionally, it is critical that the party that originally collects the unsubscribe in these cases also be held accountable, even if they did not intentionally allow for the suppression list to be misused. LashBack has seen several cases of companies where their suppression list can easily be downloaded from the web. This practice, while likely not intentional, subjects individuals who unsubscribe to even additional spam. It is absolutely critical for unsubscribe to work that parties that collect unsubscribe requests are also held accountable for misuse that occurs against that list when not taking proper security precautions to protect their suppression lists. Failure to introduce such accountability will continue to make unsubscribe a joke in the email community.